8

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/747,770	12/22/2000	Ron J. Vandergeest	0500.0008171 (10500.00.81	4395

23418 7590 09/07/2005

VEDDER PRICE KAUFMAN & KAMMHOLZ
222 N. LASALLE STREET
CHICAGO, IL 60601

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 09/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/747,770	**Applicant(s)** VANDERGEEST ET AL.	
	Examiner Thomas M. Ho	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *27-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-31 are pending.**

2. **Claims 27-31 are allowable.**

Response to Arguments

3. The Examiner has carefully considered the arguments made by the Applicant. The Examiner thanks Applicant for taking appropriate action regarding the rejection based upon 35 USC 103, obviousness. The word "anticipation" has been removed.

Applicant has argued the following on pages 11 last paragraph to page 12, first paragraph.

"In contrast, Applicants claim a different method and structure. For example, as to claim 1, the method requires sending, by a first unit, user identification data to an authentication unit and then using the user identification data sent by the first unit to determine which destination unit will receive an authentication code to be used to authenticate the user. The authentication code is then sent to the determined destination unit, the authentication code is then returned to the authentication unit and the user can then be authenticated. Crane fails to describe what is alleged in the office action. For Example, the office action states that the "application server of Figure 4" corresponds to the claimed "first unit". Taking for arguments sake, that the application server 12 in Figure 4 corresponds to the claimed "first unit", the claimed method is not met. For

example, the claim also requires using, user identification data sent by the first unit, to determine which destination unit will receive the authentication code to be used to authenticate the user. However, the office action cites that the same first unit, namely the authentication server, is the unit that both sends the authentication information and receives the sent authentication information. However, the claim requires a unit other than the first unit to perform the claimed operation since the first unit does not send information to itself."

The Examiner however disagrees with this contention. Figure 4, clearly shows five interacting units. It is evident that the Application server from figure 4 must first receive the user identification data from a user such as a client. Afterwards, the Application server, which the Examiner has mapped as the first unit both sends and receives information involving the usage of the authentication information it originally received.

Attention is directed towards the Applicant's argument.

However, the office action cites that the same first unit, ***namely the authentication server****, is the unit that both sends the authentication information and receives the sent authentication information.*

The Examiner contends Applicant's characterization is incorrect. The first unit is the application server. The authentication server, or item 17 of Figure 4, is known as the

Application authentication server, but is not the same as the Application server, which is Item 12 of Figure 4. This characterization is stated in the previous rejection

"sending, by a first unit, user identification data to an authentication unit, where the client sends via the first unit(the application server of Figure 4),"

Applicant's argument appears to maintain this view initially,

"*Taking for arguments sake, that the application server 12 in Figure 4 corresponds to the claimed "first unit","*

but then abandons it for the second part of the argument.

The Examiner contends that it is evident that when the Application server is characterized as the first unit in the claim, the authentication data is both received by the first unit, and indeed sent to several places thereafter including, the device server 12, database 15, application authentication server 17, and client 14.

As such, Applicant's arguments are unpersuasive and the previous rejection is maintained.

Applicants additional arguments appear to use the same reasoning as used in the arguments for claim 1.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-4, 6-26 are rejected under 35 U.S.C. 103(a) under Crane et al., US patent 6510236.

6. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Crane et al. US patent 6510236 and Bellare et al., US patent 5673318.

In reference to claim 1:

Crane et al. discloses a method for providing user authentication comprising:

- sending, by a first unit, user identification data to an authentication unit, where the client sends via the first unit(the application server of Figure 4), user identification data(Column 4, lines 55-63) to the authentication unit, which is the device authentication server of (Figure 4, Item 18).
- Using the user identification data sent by the first unit to determine which destination unit will receive the authentication code to authenticate the user, where the user identification data is used by the Application Server(Item 12) to access a database(Item 15) to determine which destination unit (which particular authentication server) will receive the authentication code to authenticate the user, and wherein the user identification data sent by the first unit the Application

server is used as part of the authentication process both to determine the device type and to select the application server. (Column 5, lines 1-20) et seq.

- sending the authentication code to the determined destination unit based on the user identification data, where the authentication code(code used to authenticate the client) will be sent to the destination unit(the Application authentication server, Item 17), based on user identification data. .(Column 5, lines 23-27)
- returning a response to the authentication unit (Column 5, lines 28-33)
- authenticating the user when the returned authentication code matches the sent authentication code, where the code is sent back to the user in the form of a token. (Column 5, lines 33-37)

Crane fails to explicitly disclose returning the authentication code to the authentication unit. Crane instead discloses that merely a simple yes or no is returned that digitally signed.

Crane however teaches that all of the message, or a response string may be returned instead of a digital signature. (Column 5, lines 60-64) The string, as understood the invention of Crane discloses the authentication code, which includes the user ID. (Column 4, lines 55-64)

It would have been obvious to one of ordinary skill in the art to send the string authentication code instead of a simple yes no answer in view of the fact that Crane discloses this modification to his own invention.

In reference to claim 2:

Crane et al. (Column 5, lines 35-43) discloses a method including the step of generating the authentication code on a per authentication session basis and sending the authentication code to the determined destination unit in response to the generated authentication code, where authentication code is a token generated on a per session basis through the device id.

In reference to claim 3:

Crane et al. (Column 4, line 58 – Column 5, line 27) discloses a method including the step of maintaining per user destination unit data including at least one destination unit identifier per user and wherein the step of using the user identification data to determine which destination unit will receive the authentication code includes sending the authentication code to the determined destination unit based on the stored per user destination unit identifier, where the per user destination unit identifier is the device ID, and the data of the user is maintained in a database containing userIDs matched with device IDs.

In reference to claim 4:

Crane et al. (Column 4, line 48 – Column 5, line 36) discloses a method including the step of receiving user input in response to the step of sending the authentication code and waiting to return the authentication code to the authentication unit until receipt of the user input, where after the authentication code is sent out the first time, the user enters in authentication data to be sent off to the server, and where the Authentication code isn't returned until the user gives this input.

In reference to claim 5:

The combination of Crane et al. fails to disclose a method including the steps of:

Prior to returning the authentication code to the authentication unit, digitally signing, by the first unit, the returned authentication code to produce a digitally signed authentication code that was received from the determined destination unit,

Verifying the digitally signed authentication code as part of step (e),

Crane instead discloses

Returning the authentication code to the authentication unit. (Column 5, lines 28-33) & (Column 5, lines 60-65)

Verifying the authentication code as part of step (e) (Column 5, lines 33-37)

Crane does not disclose signing this authentication code prior to sending it back.

Bellare et al. (Figure 8) discloses a method that provides security, and digitally signs the authentication code. (Column 3, lines 58-64) Bellare et al. discloses their invention allows the receiver to be confident that a message claimed to be sent by the sender was really sent by that sender (Column 3, lines 15-20), and that this method also allows forgeries to be detected. (Column 3, lines 45-50)

It would have been obvious to one of ordinary skill in the art at the time of invention to use a digital signature to sign the authentication code in order to allow forgeries in the transmission of the authentication code to be detected.

Claim 9 is rejected for the same reasons as claim 5.

Claim 10 is substantially similar to claim 1 and is rejected for the same reasons. The additional wireless back limitation is discussed in claim 15.

In reference to claim 15:

Crane et al. (Column 1, lines 25-39) & (Column 6, line 1-14) discloses a method including the step of sending the authentication code on the wireless back channel[or data based on it] to the destination unit using at least one of a short message session(SMS) channel, a paging channel and a control channel, where it is understood that a wide variety of authentication devices is supported such as biometric scanners or token cards which are frequently known in the art to operate based on a RF (radio frequency) transmission.

In reference to claim 16:

Crane et al. (Column 5, lines 14-36) discloses a method including the step of validating the primary authentication information, where the device authentication server validates the primary authentication information.

Claims 17, 6 are rejected for the same reasons as claim 1.

Claims 22, 18, 11, 7 are rejected for the same reasons as claim 2.

Claims 23, 19, 12, 8 are rejected for the same reasons as claim 3.

Claims 24, 13 are rejected for the same reasons as claim 4.

Claims 25, 14 are rejected for the same reasons as claim 5.

Claim 20 is rejected for the same reasons as claim 9.

Claim 26 is rejected for the same reasons as claim 15.

Reasons for Allowance

7. The following discloses Examiner's reasons for allowance of claims 27-31.

In reference to claim 27:

Crane et al. (Column 4, line 48 – Column 5, line 53) discloses a system for providing user authentication comprising:

- A first unit, where the first unit is the authentication device of the client.
- A second unit operatively coupleable to the first unit via a primary wireless channel and operatively coupleable to an authenticator, where the second unit is the application server of figure 4, and where the primary wireless channel is the wireless channel connecting the application server, with a wireless authentication device(biometric scanner, token reader (Column 3, lines 10-37)) of the client. (Figure 1, Items 16, 14)

- A third unit, operatively coupleable to the second unit where the third unit is the device authentication server (Figure 4, Item 18), and the second device is the application server. (Figure 4, Item 12)
- The first unit operative to send primary authentication information via the primary channel during a session to the second unit, where the authentication information is the authentication string(Column 4, lines 52-64), and the first unit is the client, the second is the application server of (Figure 4)
- The authenticator operative to use the primary authentication information to determine which destination unit, other that the first unit, will receive an authentication code as a secondary authentication information via the wireless back channel and wherein the destination unit is the third unit, where the authenticator is the database device, (Item 15 of Figure 4), which goes and uses the authentication information to determine which destination unit(device server 18 of Figure 4) will receive the an authentication code.
- The second unit operative to the send the authentication code to the destination unit based on the primary authentication information sent via the primary channel during the same session (Figure 4, Item 2)

Crane et al fails to disclose the uses of a wireless connection between the second device and the third device. However, the Examiner notes that the use of wireless connections to connect one digital system to another is ubiquitous and has been in use at in radios since at least World War II. Other common embodiments include cell phones, wireless LANs, CBs, and PDAs. It would have been obvious to one of ordinary skill in the art at the time of invention to employ the use of wireless connections between the servers in order to provide the advantage of not having to purchase and maintain wires between them, and the provide the advantage of portability.

Crane also fails to explicitly **a direct** embodiment in which

- The authenticator operative to authenticate the user which the returned authentication code received from the wireless primary channel matches the sent authentication code that was sent.

Crane discloses directly that the authenticator returns a Y/N which is signed (Item 3, Figure 4) instead of an authentication code.

Crane however later discloses that a modification can be made to his device in which rather than sending a digital signature, a "String" may be returned. (Column 5, line 60-64). Crane defines a string in his invention to include the userid and device type among other authentication data. (Column 4, lines 52-63) These two pieces of information comprise the authentication code.

Because of this disclosure, the Examiner considers a modification in which Item 3, was modified to return the authentication string or (code) to be obvious in view of Crane. In other words, Crane with the modification mentioned discloses a method in which the authenticator, operative to authenticate the user(client) which the returned authentication code received from the wireless primary channel. (authentication device of client, Item 16, Figure 1) matches the authentication code that was sent. (Item 1, Figure 4)

No art can be found however that discloses a system for providing authentication in which

- The first unit operative to return the authentication code on the wireless primary channel to the second unit during the same session

The Examiner notes that while in the art, it is known that a client(first unit) with an authentication code, may send an acknowledgment of receipt, or an acknowledgement of integrity for the code to a second unit,

no art nor motivation to combine can be found in which the first unit(**abiding by the claimed limitations set forth in Claim 27**) would return the authentication code to the second unit during the same session.

For this reason, Claim 27 and its dependent claims are allowable.

Conclusion

8. The following art not relied upon is made of record:

- Kung, US patent 5241594 discloses a one time logon means in a distributing computing context.

9. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of the final action and the advisory action is not mailed under after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension pursuant to 37 CFR 1.136(A) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 703-872-9306
Customer Service Representative	Telephone: 571-272-2100	Fax: 703-872-9306

TMH

September 3rd, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100